ВСЕРОССИЙСКОЕ
ЧЕМПИОНАТНОЕ
ДВИЖЕНИЕ
ПО ПРОФЕССИОНАЛЬНОМУ
МАСТЕРСТВУ

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

по категории «Юниоры»

2023 г.

Конкурсное задание разработано экспертным сообществом и утверждено Менеджером компетенции.

В настоящем конкурсном задании установлены правила и необходимые требования владения профессиональными навыками для участия в соревнованиях по профессиональному мастерству, применяемы к категории «Юниоры».

Конкурсное задание включает в себя следующие разделы:

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

1. ИКС – Информационно коммуникационная система
2. КС – Компьютерная сеть
3. ОС – Операционная система
4. КЗ – конкурсное задание

1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ

1.1. ОБЩИЕ СВЕДЕНИЯ О ТРЕБОВАНИЯХ КОМПЕТЕНЦИИ

Требования компетенции (ТК) «Сетевое и системное администрирование» определяют знания, умения, навыки и трудовые функции, которые лежат в основе наиболее актуальных требований работодателей отрасли, применяемые к категории «Юниоры».

Целью соревнований по компетенции является демонстрация лучших практик и высокого уровня выполнения работы по соответствующей рабочей специальности или профессии, применяемых в категории «Юниоры».

Требования компетенции являются руководством для подготовки конкурентоспособных, высококвалифицированных специалистов/рабочих и участия их в конкурсах профессионального мастерства, применяемые в категории «Юниоры».

В соревнованиях по компетенции проверка знаний, умений, навыков и трудовых функций осуществляется посредством оценки выполнения практической работы.

Требования компетенции разделены на четкие разделы с номерами и заголовками, каждому разделу назначен процент относительной важности, сумма которых составляет 100.

1.2. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ СПЕЦИАЛИСТА ПО КОМПЕТЕНЦИИ «Сетевое и системное администрирование»

Таблица №1. Перечень профессиональных задач специалиста.

№ п/п	Раздел	Важность в %
1	Выполнение работ по выявлению и устранению инцидентов в информационно-коммуникационных системах	25
	- Специалист должен знать и понимать: Лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения Основы архитектуры, устройства и функционирования вычислительных систем Принципы организации, состав и схемы работы операционных систем Стандарты информационного взаимодействия систем	

	Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе Инструкции по установке администрируемых сетевых устройств Инструкции по эксплуатации администрируемых сетевых устройств Инструкции по установке администрируемого программного обеспечения Инструкции по эксплуатации администрируемого программного обеспечения Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.	
	- Специалист должен уметь: Идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки Оценивать степень критичности инцидентов при работе прикладного программного обеспечения Устранять возникающие инциденты Локализовать отказ и инициировать корректирующие действия Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий Производить мониторинг администрируемой информационно-коммуникационной системы Конфигурировать операционные системы сетевых устройств Пользоваться контрольно-измерительными приборами и аппаратурой Документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику	
2	Обеспечение работы технических и программных средств информационно-коммуникационных систем	25
	- Специалист должен знать и понимать Использовать современные методы контроля производительности информационно-коммуникационной системы; Анализировать сообщения об ошибках в сетевых устройствах и операционных системах;	

	Локализовывать отказ и инициировать корректирующие действия; Применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств; Применять штатные программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы; Применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы;	
	- Специалист должен уметь: Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети; Инструкции по установке администрируемых сетевых устройств; Инструкции по эксплуатации администрируемых сетевых устройств; Инструкции по установке администрируемого программного обеспечения; Инструкции по эксплуатации администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Базовая эталонная модель взаимодействия открытых систем; Международные стандарты локальных вычислительных сетей; Модели информационно-телекоммуникационной сети «Интернет»; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Устройство и принцип работы кабельных и сетевых анализаторов; Средства глубокого анализа информационно-коммуникационной системы; Метрики производительности администрируемой информационно-коммуникационной системы; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы;	

3	Реализация схемы резервного копирования, архивирования и восстановления конфигураций технических и программных средств информационно-коммуникационных систем по утвержденным планам	25
	- Специалист должен знать и понимать: Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; Инструкции по установке администрируемых сетевых устройств информационно-коммуникационной системы; Инструкции по эксплуатации администрируемых сетевых устройств информационно-коммуникационной системы; Инструкции по установке администрируемого программного обеспечения; Инструкции по эксплуатации администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Базовая эталонная модель взаимодействия открытых систем для управления сетевым трафиком; Международные стандарты локальных вычислительных сетей Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы;	
	- Специалист должен уметь: Использовать процедуры восстановления данных; определять точки восстановления данных; работать с серверами архивирования и средствами управления операционных систем; Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; Выполнять плановое архивирование программного обеспечения пользовательских устройств согласно графику;	

4	Внесение изменений в технические и программные средства информационно-коммуникационных систем по утвержденному плану работ	25
	- Специалист должен знать и понимать: Использовать современные методы контроля производительности информационно-коммуникационной системы; Анализировать сообщения об ошибках в сетевых устройствах и операционных системах; Локализовывать отказ и инициировать корректирующие действия; Применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств; Применять штатные программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы; Применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы;	
	- Специалист должен уметь: Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети; Инструкции по установке администрируемых сетевых устройств; Инструкции по эксплуатации администрируемых сетевых устройств; Инструкции по установке администрируемого программного обеспечения; Инструкции по эксплуатации администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Базовая эталонная модель взаимодействия открытых систем; Международные стандарты локальных вычислительных сетей; Модели информационно-телекоммуникационной сети «Интернет»; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Устройство и принцип работы кабельных и сетевых анализаторов; Средства глубокого анализа	

	информационно-коммуникационной системы; Метрики производительности администрируемой информационно-коммуникационной системы; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы;	

1.3. ТРЕБОВАНИЯ К СХЕМЕ ОЦЕНКИ

Сумма баллов, присуждаемых по каждому аспекту, должна попадать в диапазон баллов, определенных для каждого раздела компетенции, обозначенных в требованиях и указанных в таблице №2.

Таблица №2

Таблица №2. Матрица пересчета требований компетенции в критерии оценки.

		Критерий/Модуль					Итого баллов за раздел ТРЕБОВАНИЙ КОМПЕТЕНЦИИ
		А	Б	В	Г	Д	
Разделы ТРЕБОВАНИЙ КОМПЕТЕНЦИИ	1	2	5	2	2	5	20
	2	2	5	2	2	5	20
	3	3	10	3	3	10	30
	4	3	10	3	3	20	30
Итого баллов за критерий/модуль		10	30	10	10	40	**100**

1.4. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ

Оценка Конкурсного задания будет основываться на критериях, указанных в таблице №3:

Таблица №3. Оценка конкурсного задания.

Критерий		Методика проверки навыков в критерии
А	**Аудит**	Определяется в соответствии с используемыми ОС и сетевым оборудованием
Б	**Настройка технических и программных средств информационно-коммуникационных систем**	Определяется в соответствии с используемыми ОС и сетевым оборудованием
В	**Обеспечение отказоустойчивости**	Определяется в соответствии с используемыми ОС и сетевым оборудованием
Г	**Миграция**	Определяется в соответствии с используемыми ОС и сетевым оборудованием
Д	**Автоматизация**	Определяется в соответствии с используемыми ОС и сетевым оборудованием

1.5. КОНКУРСНОЕ ЗАДАНИЕ

Общая продолжительность КЗ: 8 ч.

Количество конкурсных дней: 2 дня.

КЗ включает оценку по каждому из разделов требований компетенции.

Оценка знаний участника проводится через практическое выполнение КЗ.

1.5.1. Разработка/выбор конкурсного задания

КЗ состоит из 2 модулей. Для выполнения КЗ неизменным является модуль Б. В качестве вариативного модуля выбран модуль Д. Общее количество баллов настоящего КЗ составляет 100.

Матрица конкурсного задания приведена в Приложении №1.

1.5.2. Структура модулей конкурсного задания

Модуль А. (*Аудит*)

Время на выполнение модуля

Задания:

На текущем чемпионате модуль не применяется

Модуль Б. (*Настройка технических и программных средств информационно-коммуникационных систем*)

Время на выполнение модуля 4 часа

Задание:

Однажды, в одном дальнем-дальнем восточном регионе команда из двух юных, но достаточно компетентных системных администраторов взялась за проект организации сетевой и серверной инфраструктуры для ООО «СибИгрСтрой» з – небольшой, но перспективной компании по разработке игровых модов и хостингу игровых серверов.

На текущий момент в организации имеется два офиса, в городах Красноярск (внутреннее обозначение KJA) и Владивосток (VVO) и виртуальный сервер в интернете с кодовым названием VDS. Все данное оборудование в филиалах только что распаковано, операционные системы предустановлены, дополнительную информацию о предустановленном ПО можно найти в разделах предоставленного вам для работы технического задания. Для широкополосного доступа к сети Интернет нашей компанией заключены договора с провайдерами интернета для обоих филиалов с предоставлением «белых» ip-адресов *(подробнее про сети провайдеров в разделе «Техническое описание лабораторной инфраструктуры и общие требования к реализации»).

Также, у нас есть пара постоянных клиентов в городах Омск и Иркутск, которые с радостью предоставят нам свои компьютеры ClientOMS и ClientIKT для тестирования удаленного доступа к великолепным сервисам нашей компании.

В случае, если в тексте задания не указано иное, все пользовательские учетные записи должны иметь пароль P@ssw0rd.

При выполнении настоящего задания всегда нужно руководствоваться правилом наименьших привилегий.

Обратите внимание, что провайдерская адресация 100.64.0.0/10 относится к серому (частотному) диапазону адресов, что может потребовать дополнительных настроек на граничных сетевых устройствах межсетевого экранирования. Однако, в терминологии задания, сеть 100.64.0.0/10 относится к внешним («белым») сетям, наряду с «белыми» сетями из реального интернета.

Знак * (звёздочка, астериск) в задании является подстановочным знаком заменяет произвольную последовательность символов от начала строки или пробельного символа до другого пробельного символа или конца строки. К примеру, при указании на устройство FW* имеются ввиду все устройства в задании, название которых начинается с FW, например FW1, FW-MSK, FWabc и т.п., а при указании сетей *MSK имеются в виду все сети в задании, название которых заканчивается на MSK, например LAN1-MSK, SRV-MSK, dmzMSK и т.п.

1 день – Настройка инфраструктуры в головном офисе компании.

1. Настройте статические IPv4-адреса, шлюз по умолчанию и описания на интерфейсах FW* и R0 согласно схеме адресации.
2. Настройте статические IPv4-адреса и шлюз по умолчанию на всех устройствах, где это требуется, согласно схеме адресации.
3. Настройте интерфейсы loopback на всех FW* и R*.
4. Настройте имена всех устройств согласно топологии.
5. Настройте OSPFv2 между R0-KJA и FW-KJA
   - 5.1. FW-KJA должен узнавать о сети SRV-KJA через OSPF.
   - 5.2. R0 должен получать маршрут по умолчанию и другие необходимые маршруты от FW-KJA через OSPF.
   - 5.3. Не используйте статические маршруты до этих сетей. Статические маршруты применимы только в качестве временной меры.
   - 5.4. Маршруты до loopback интерфейсов также должны распространяться по OSPF.
   - 5.5. R0-KJA должен быть защищен от вброса маршрутов с интерфейсов смотрящих в сторону сетей SRV-KJA.
   - 5.6. FW-KJA должен быть защищен от вброса маршрутов с интерфейса смотрящего в сторону сети DMZ-KJA.

6. Все устройства в филиалах Красноярска и Владивостока должны иметь доступ в интернет, если в задании явно не указано иного.
7. В филиале VVO разверните домен vvo.jun.profi на базе FreeIPA с контроллером домена на сервере SRV-VVO. При развертывании учтите, что это устройство также будет выполнять функции DNS и DHCP сервера в филиале VVO. Также, выполните следующие действия в развернутом домене:
    7.1. Создайте пользователей den и alex, поместите их в группу jun-users
    7.2. создайте правило, разрешающее пользователю admin использовать sudo на всех компьютерах в домене без ограничения.
    7.3. обеспечьте доменному пользователю admin, после успешной авторизации на компьютере PC-VVO, возможность заходить в интерфейс FreeIPA без использования пароля. Для аутентификации и авторизации используйте Kerberos.
    7.4. Создайте обратную зону(ы) DNS в доменном DNS-сервере, чтобы все адреса в филиале VVO, кроме сети GUEST-VVO, расшифровывались в соответствующие им имена.
8. Настройте инфраструктуру разрешения имен в филиалах следующим образом:
    8.1. DNS-сервер в филиале KJA располагается на FW-KJA.
    8.2. DNS-сервер в филиале VVO располагается на SRV-VVO и интегрирован с доменом FreeIPA.
    8.3. Все устройства в локальных сетях должны обращаться с DNS запросами к указанным выше DNS-серверам
    8.4. Указанные DNS-сервера должны выполнять пересылку DNS запросов от локальных клиентов на DNS сервер по адресу 100.100.100.100.
    8.5. Client* и VDS должны обращаться с DNS запросами к 100.100.100.100.
    8.6. Настройте для всех устройств филиалов в Красноярске и Владивостоке доменные имена в зонах kja.jun.profi и vvo.jun.profi соответственно.
    8.7. Все устройства должны быть доступны в локальных сетях всех филиалов по именам в соответствии с топологией в доменах соответствующих филиалов. К примеру srv1-kja.kja.jun.profi или pc-vvo.vvo.jun.profi
    8.8. В рамках каждого филиала короткие имена должны автоматически дополняться доменным именем соответствующего филиала

9. Настройте DHCP-сервер на FW-KJA для клиентов сети LAN-KJA, а также на SRV-VVO для клиентов сетей LAN-VVO и GUEST-VVO. DHCP-сервер должен передавать клиентам все необходимые опции для работы в сети и взаимодействия с другими устройствами и сетями по IP и DNS именам.
    9.1. Выдаваемый диапазон адресов должен иметь запас в как минимум по 10 свободных адресов в начале и конце сети, но не более 50 суммарного запаса.
10. Настройте необходимые параметры на устройстве FW-VVO таким образом, чтобы клиентам в сети LAN-VVO и GUEST-VVO адреса выдавал сервер SRV-VVO.
11. Настройте синхронизацию времени
    11.1. Сервер точного времени в филиале KJA располагается на SRV-VVO.
    11.2. Сервер точного времени в филиале VVO располагается на FW-VVO.
    11.3. Все устройства в локальных сетях должны использовать указанные сервера.
    11.4. Все сервера и клиенты, которые поддерживают Chrony должны использовать данную реализацию протокола. На устройствах, которые не поддерживают Chrony допускается использовать стандартный NTP.
    11.5. Указанные сервера времени, а также сервера и клиенты во внешних сетях должны синхронизировать свое время с NTP сервером по адресу 100.101.102.103.
    11.6. Настройте часовой пояс на всех устройствах в соответствии с их географическим расположением.
12. Установите пользователю PC-VVO Яндекс Браузер. Для удобства работы создайте для него ярлык на рабочем столе.
13. Настройте правила межсетевого экранирования так, чтобы устройства в сетях DMZ-* не могли инициировать соединения к клиентам в приватных сетях организации, при этом входящие соединения из всех локальных сетей в сети DMZ-* должны быть разрешены и машины в сети DMZ-* должны иметь доступ в интернет. При необходимости, допускается возможность штучно открывать дополнительные порты, необходимые для выполнения задания.
14. Настройте сетевое обнаружение по протоколу LLDP на всех сетевых устройствах и серверах в локальных сетях.
    14.1. Информация протокола LLDP ни в коем случае не должна передаваться во внешние сети. (это в 30%)

15. Настройте защищенный VPN-туннель FW-AMS<=>FW-KJA со следующими параметрами:
    15.1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.
    15.2. Используйте современные надежные протоколы шифрования AES и SHA-2
    15.3. Не допускается использование протоколов шифрования и аутентификации с длиной ключа/хеша менее 256 бит.
    15.4. Настройте маршрутизацию, NAT и межсетевой экран таким образом, чтобы трафик для другого офиса не натировался и не блокировался
16. Настройте работу OSPF между R* и FW*, чтобы все маршрутизаторы имели полную информацию о маршрутов во все локальные сети всех филиалов.
17. Настройте централизованный сбор журналов syslog на SRV-KJA.
    17.1. Журналы должны храниться в файлах /opt/logs/[hostname], где hostname - это короткое или полное доменное имя машины, предоставившей соответствующие сообщения.
    17.2. R0-KJA должен записывать только сообщения error и более важные.
    17.3. SRV-KJA и APP-KJA должны записывать только сообщения warning и более важные.
    17.4. FW должен записывать сообщения от служб ospf и имеющихся на устройстве служб туннелирования (ipsec, openvpn, wireguard и т.д) уровня не менее notice; если служба туннелирования не имеет своей категории логов, то должны записываться все события интерфейсов уровня не менее notice.

Модуль В. (*Обеспечение отказоустойчивости*)

Время на выполнение модуля

Задания:

На текущем чемпионате модуль не применяется

Модуль Г. (*Миграция*)

Время на выполнение модуля

Задания:

На текущем чемпионате модуль не применяется

Модуль Д. (*Автоматизация*)

Время на выполнение модуля 4 часа

Задание:

2 день – Настройка удаленного доступа и автоматизация сетевых сервисов компании.

1. Настройте CA на SRV-KJA со следующими параметрами
   1.1. Используйте /opt/ca в качестве корневой директории CA.
   1.2. Страна: RU;
   1.3. Организация: JUN PROFI
   1.4. CN должен быть установлен как JUN PROFI CA.
   1.5. Создайте корневой сертификат CA.
   1.6. SRV-KJA и PC-KJA должны доверять CA.
2. На сервере SRV1-KJA должен быть развернут WEB-сервер корпоративного портала организации:
   2.1. Файлы сайта должны располагаться в директории /var/www/portal
   2.2. Сайт должен открываться по адресу corp.jun.profi
   2.3. Обращение к сайту из внутренних сетей организации должно происходить только по внутренним каналам связи, однако сайт должен также быть доступен и внешним клиентам по тому же адресу.
   2.4. Сайт должен содержать следующий текст “Welcome to secure corporate portal jun.profi”
   2.5. Сайт должен функционировать по протоколу HTTPS. При обращении по протоколу HTTP должен происходить автоматический редирект на HTTPS.
   2.6. WEB-сервер должен иметь сертификат, подписанный корпоративным центром сертификации
   2.7. Сайт должен открываться с PC-KJA без ошибок и предупреждений.
   2.8. Для работоспособности портала из внешнего мира, передайте необходимые настройки хостинг-провайдеру.
3. Создайте пользователя admin на APP-KJA, и добавьте его в группу ftpusers.
4. Настройте права доступа для каталога /var/www на APP-KJA следующим образом:

4.1. пользователь admin должен иметь полные права на чтение и запись в указанный каталог и все его подкаталоги.
4.2. обычные пользователи не должны иметь прав на запись в данный каталог
4.3. службы настроенного ранее веб-сервера должны иметь необходимые права для работы сайта.

5. Настройте общий доступ к файлам на APP-KJA по протоколу FTP.
   5.1. Доступ должен быть только у пользователей группы ftpusers.
   5.2. FTP-сервер должен предоставлять доступ только к содержимому папки /var/www/ и вложенных в нее папок.
   5.3. Доступ к FTP-серверу должен быть только у клиентов сети LAN-KJA
6. Настройте клиент FTP на PC-KJA.
   6.1. Установите ПО Filezilla актуальной стабильной версии и проверьте возможность подключения к корпоративному FTP-серверу.
   6.2. Обеспечьте монтирование корпоративного FTP-хранилища на PC-KJA в папку /opt/ftp/
   6.3. Монтирование должно восстанавливаться при перезагрузке виртуальной машины.
7. Обеспечьте веб-интерфейс FW-KJA сертификатом HTTPS, подписанным корпоративным центром сертификации, обеспечивающим доверенное соединение при обращении к FW-KJA по полному и сокращенному DNS-имени с PC-KJA.
8. Обеспечьте возможность подключения к FW-KJA под пользователем admin:
   8.1. посредством веб-интерфейса с полным доступом к настройкам
   8.2. посредством протокола SSH с доступом к выполнению команд через sudo
   8.3. при подключении с компьютера PC-KJA авторизация SSH должна осуществляться по ключу без необходимости ввода пароля
9. Настроить удаленный доступ к VDS и R0-KJA по SSH
   9.1. Устройство PC-KJA при входе под пользователем user должно иметь доступ к VDS под пользователем user с использованием SSH ключей, без необходимости ввода пароля.
   9.2. Пользователь user на VDS должен иметь возможность выполнять команды через sudo без ввода пароля.

9.3. Подключение к VDS с PC-KJA должно осуществляться по имени “VDS”
9.4. Устройство PC-KJA при входе под пользователем user должно иметь доступ к R0-KJA под пользователем vyos с использованием SSH ключей, без необходимости ввода пароля.

10. Обеспечьте подключение клиента ClientIKT к серверу VPN на FW-KJA.
    10.1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.
    10.2. Клиент должен иметь доступ к серверам в сети SRV-KJA и DMZ-KJA.
    10.3. Соединение должно автоматически устанавливаться при включении компьютера или входе под пользователем user.
11. Обеспечьте подключение удаленного сотрудника с компьютера ClientIKT к корпоративному порталу https://corp.jun.profi следующим образом:
    11.1. посредством VPN-подключения, когда оно активно.
    11.2. посредством доступа по внешнему адресу, когда vpn-соединение неактивно.
    11.3. Открытие портала не должно вызывать ошибок и предупреждений безопасности.
12. Для хранения важных данных в сервер VDS установлено два дополнительных диска. Объедините их в RAID1 используя технологию md raid. На полученном резервированном носителе создайте файловую систему ext4 и подключите раздел по пути /opt/mc/data для дальнейшего использования.
13. На VDS разверните сервер Minecraft со следующими параметрами:
    13.1. Имя сервера: Jun Profi
    13.2. Ограничение кол-ва игроков: 12
    13.3. Порт: по умолчанию
    13.4. Проверка аккаунтов пользователей: отключена
    13.5. Сервер должен быть запущен в виде контейнера Docker
    13.6. Данные сервера должны храниться по пути /opt/mc/data/
    13.7. Контейнер должен автоматически запускаться после перезагрузки компьютера
14. Помогите постоянному клиенту из Омска подготовить рабочее место ClientOMS:
    14.1. Установите tlauncher. Обязательно создайте ярлык установленного tlauncher на рабочем столе пользователя, чтобы ему было удобнее подключаться к Вашему серверу.

14.2. Установите OBS последней стабильной версии посредством системы управления пакетами Flatpak. Обязательно создайте ярлык установленного OBS на рабочем столе пользователя, чтобы ему было удобнее запускать стрим игры на Вашем сервере.

15. На сервере DMZ-AMS разверните сервер облачного хранения данных со следующими параметрами:
    15.1. Файловый сервер: NextCloud
    15.2. База данных: MariaDB
    15.3. Веб интерфейс БД: phpMyAdmin
    15.4. Порт NextCloud: 80
    15.5. Порт phpMyAdmin: 8888
    15.6. Все сервисы должны быть запущены в виде контейнеров Docker
    15.7. Все контейнеры должны автоматически запускаться после перезагрузки компьютера
    15.8. Обеспечьте работоспособность сервера и возможность входа под пользователем user.
16. Обеспечьте возможность сохранения конфигурации FW-KJA на развернутое хранилище NextCloud в директорию opns-backup, под пользователем user посредством веб-интерфейса FW-KJA.
    16.1. Настройте автоматическое сохранение конфигурации в указанное расположение каждые 12 минут.
17. Обеспечьте возможность удаленным сотрудникам, подключенным к корпоративному VPN-сервису, использовать корпоративное облачное хранилище.

2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ

1. Участникам при выполнении всех модулей нельзя использовать интернет-ресурсы.
2. Участники имеют право задавать уточняющие вопросы экспертам (кроме эксперта наставника) и вправе получить ответ, если вопрос не предполагает получения информации о реализации конкретной технологии.

2.1. Личный инструмент конкурсанта

Нулевой - нельзя ничего привозить.

2.2. Материалы, оборудование и инструменты, запрещенные на площадке

Мобильные устройства, устройства фото-видео фиксации, носители информации.

3. Приложения

Приложение №1. Матрица конкурсного задания.

Приложение №2 Критерии оценки.

Приложение №3 Инструкция по охране труда и технике безопасности по компетенции «Сетевое и системное администрирование».

Приложение № 5 Чертежи, технологические карты, алгоритмы, схемы и т.д.